

ECSAV8^{Q&As}

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/ecsav8.html>

100% Passing Guarantee
100% Money Back Assurance

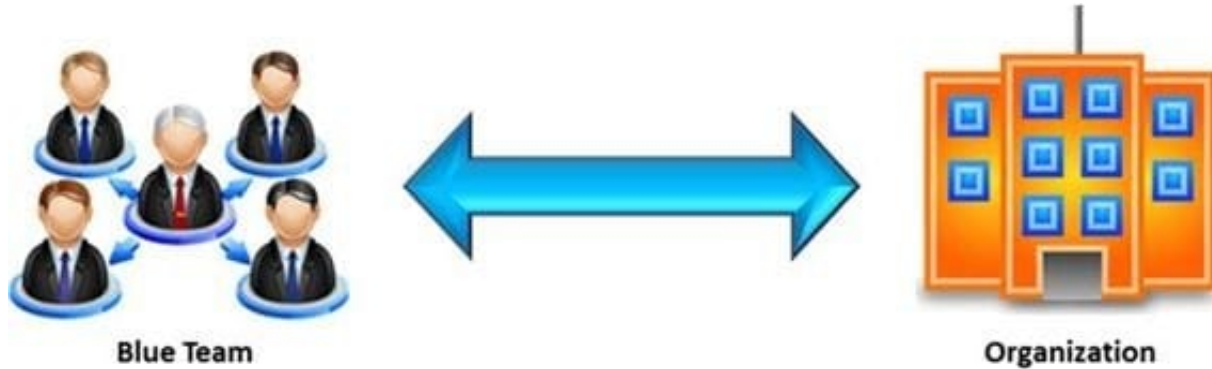
Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

In the context of penetration testing, what does blue teaming mean?



- A. A penetration test performed with the knowledge and consent of the organization's IT staff
- B. It is the most expensive and most widely used
- C. It may be conducted with or without warning
- D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Correct Answer: A

Reference: <https://www.sypriselectronics.com/information-security/cyber-security-solutions/computernetwork-defense/>

QUESTION 2

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructions, encryption used, and web page behaviors?



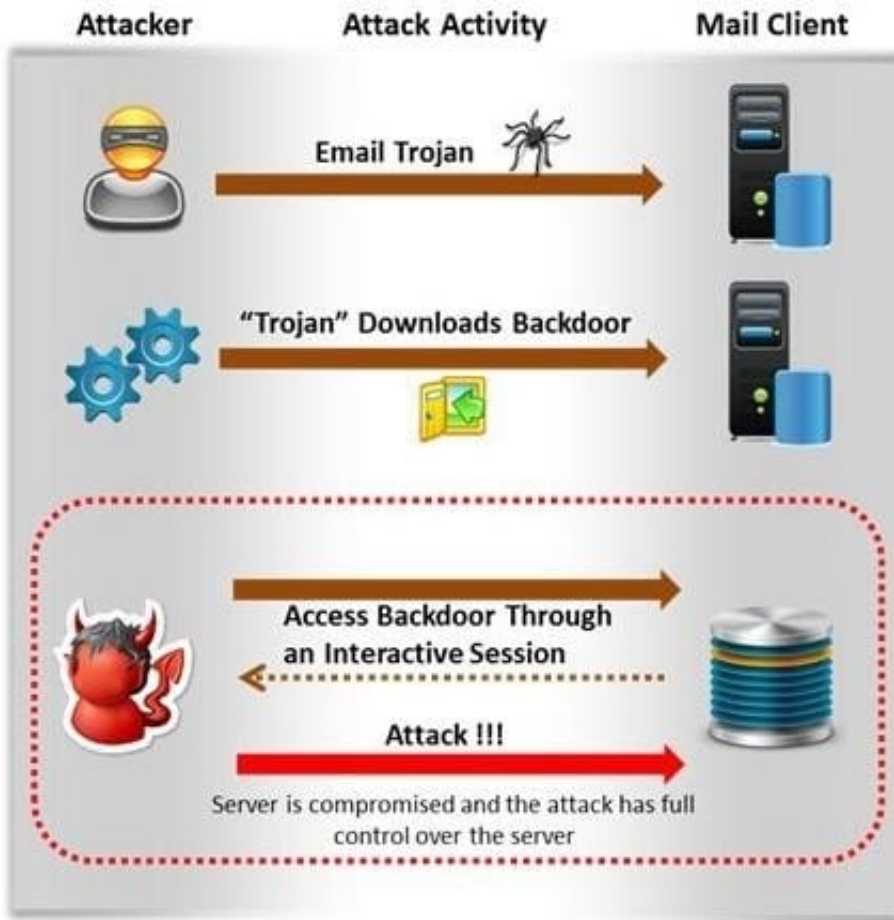
- A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
- B. Examine Server Side Includes (SSI)
- C. Examine Hidden Fields
- D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C

Reference: <http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction> (page 71)

QUESTION 3

Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

- A. Internal network mapping to map the internal network of the target machine
- B. Port scanning to determine what ports are open or in use on the target machine
- C. Sniffing to monitor all the incoming and outgoing network traffic
- D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D

QUESTION 4

Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.



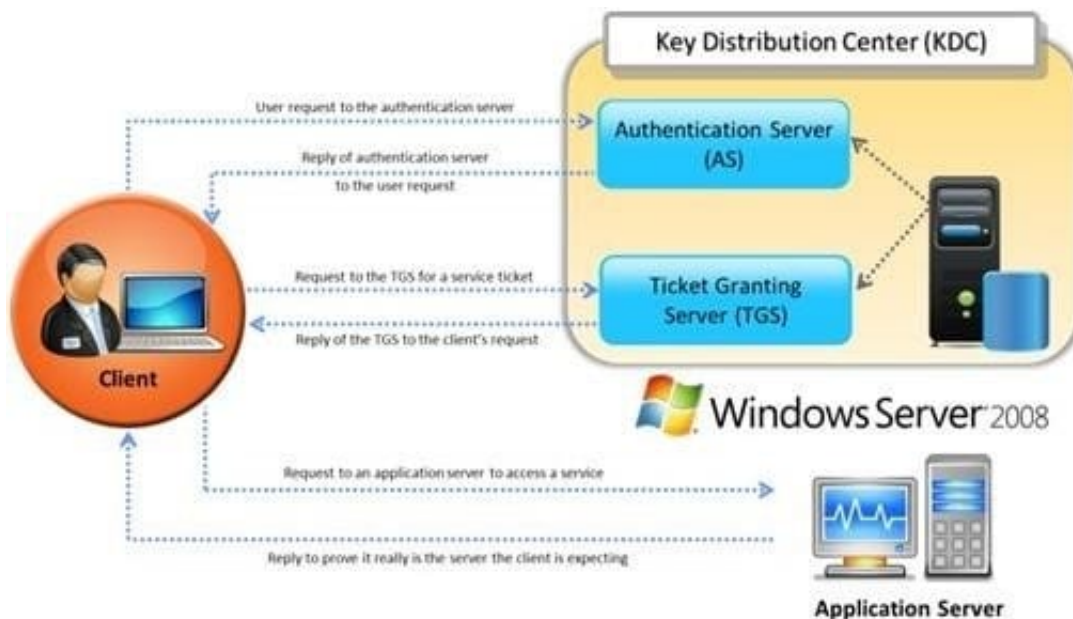
Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

- A. Web Penetration Testing
- B. Functionality Testing
- C. Authorization Testing
- D. Source Code Review

Correct Answer: D

QUESTION 5

Identify the type of authentication mechanism represented below: A. NTLMv1



- B. NTLMv2
- C. LAN Manager Hash
- D. Kerberos

Correct Answer: D

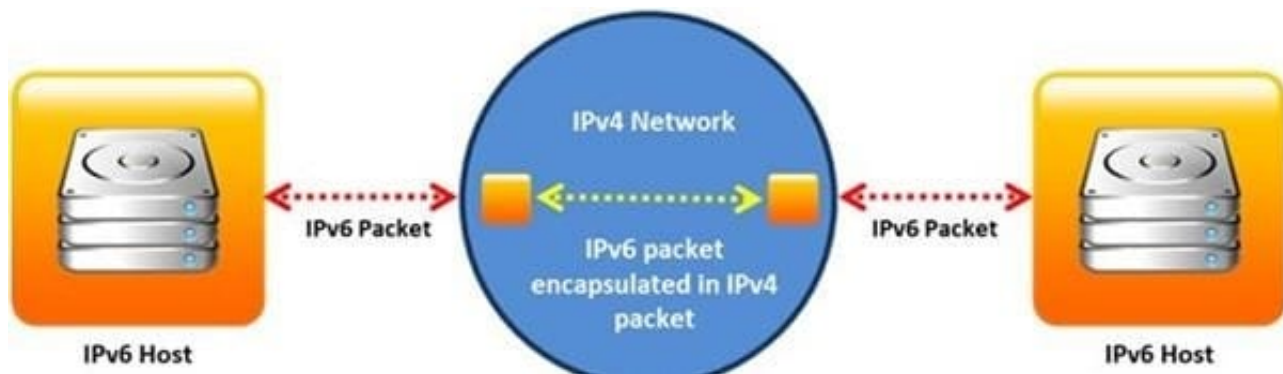
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: [http://en.wikipedia.org/wiki/Kerberos_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))

QUESTION 6

Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.

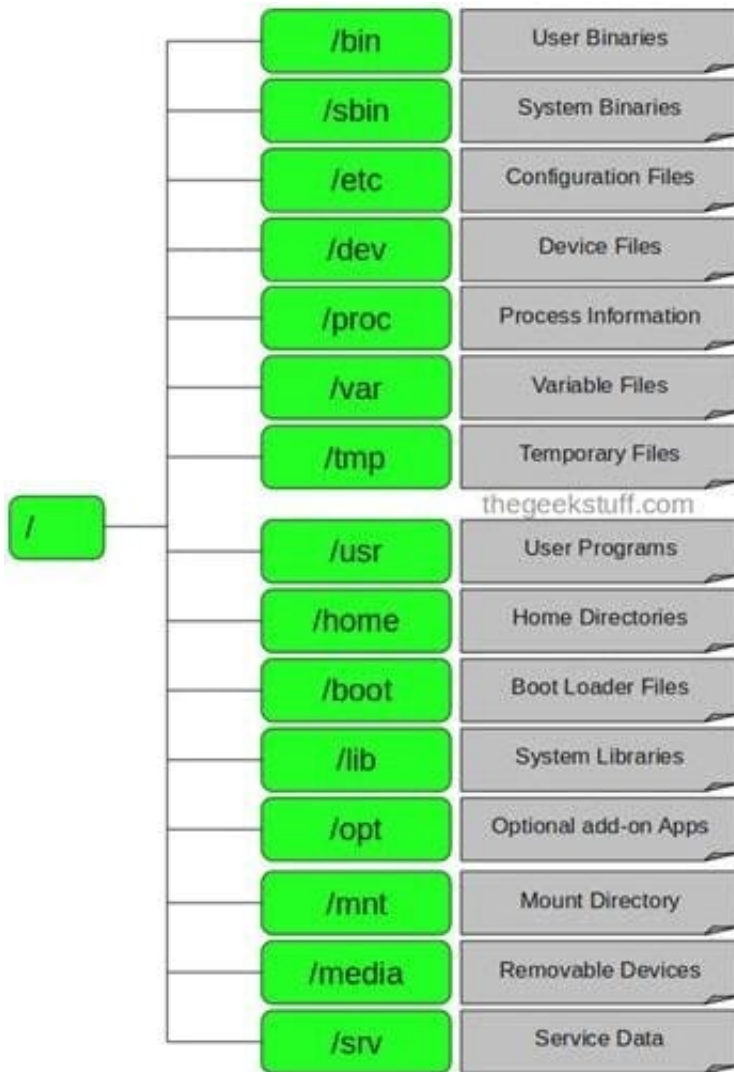


- A. Translation
- B. Tunneling
- C. Dual Stacks
- D. Encapsulation

Correct Answer: D

QUESTION 7

In Linux, `/etc/shadow` file stores the real password in encrypted format for user's account with added properties associated with the user's password.



In the example of a /etc/shadow file below, what does the bold letter string indicate? Vivek:
`1fnffc$GteyHdicpGOffXX40w#5:13064:0:99999:7`

- A. Number of days the user is warned before the expiration date
- B. Minimum number of days required between password changes
- C. Maximum number of days the password is valid
- D. Last password changed

Correct Answer: B

Reference: <http://www.cyberciti.biz/faq/understanding-etcshadow-file/> (bullet # 4)

QUESTION 8

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

- A. Decreases consumed employee time and increases system uptime

- B. Increases detection and reaction time
- C. Increases response time
- D. Both a and c

Correct Answer: A

Reference: <http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems> (economic advantages, first para)

QUESTION 9

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

- A. Techniques for data collection from systems upon termination of the test
- B. Techniques for data exclusion from systems upon termination of the test
- C. Details on how data should be transmitted during and after the test
- D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 10

Which of the following defines the details of services to be provided for the client's organization and the list of services required for performing the test in the organization?

- A. Draft
- B. Report
- C. Requirement list
- D. Quotation

Correct Answer: D

QUESTION 11

Which of the following attacks is an offline attack?

- A. Pre-Computed Hashes
- B. Hash Injection Attack
- C. Password Guessing
- D. Dumpster Diving

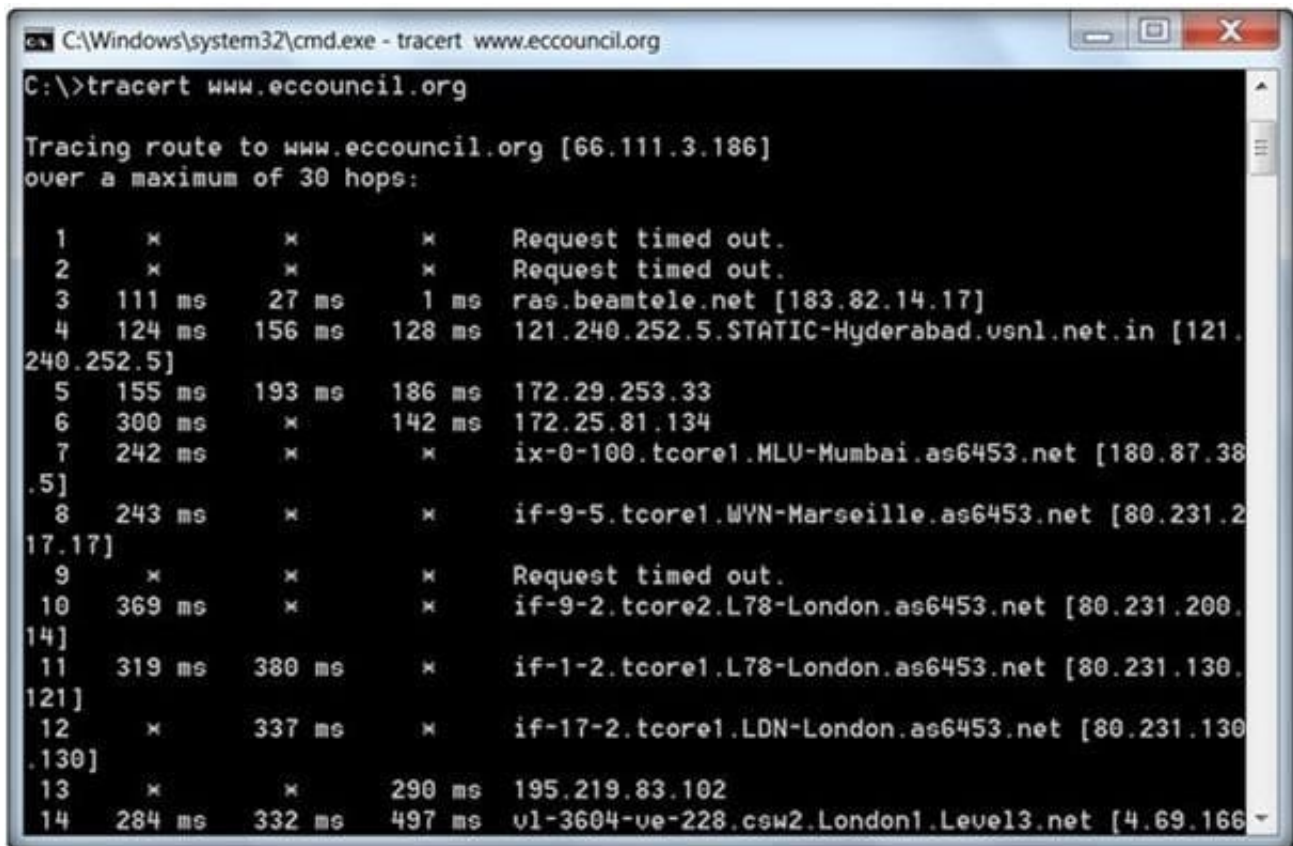
Correct Answer: A

Reference: <http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html>

QUESTION 12

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



```
C:\Windows\system32\cmd.exe - tracert www.eccouncil.org
C:\>tracert www.eccouncil.org

Tracing route to www.eccouncil.org [66.111.3.186]
over a maximum of 30 hops:

  0  *         *         *         Request timed out.
  1  *         *         *         Request timed out.
  2  111 ms    27 ms     1 ms     ras.beamtele.net [183.82.14.17]
  3  124 ms    156 ms    128 ms   121.240.252.5.STATIC-Hyderabad.usn1.net.in [121.240.252.5]
  4  155 ms    193 ms    186 ms   172.29.253.33
  5  300 ms    *         142 ms   172.25.81.134
  6  242 ms    *         *         ix-0-100.tcore1.MLU-Mumbai.as6453.net [180.87.38.5]
  7  243 ms    *         *         if-9-5.tcore1.WYN-Marseille.as6453.net [80.231.200.17.17]
  8  *         *         *         Request timed out.
  9  369 ms    *         *         if-9-2.tcore2.L78-London.as6453.net [80.231.200.14]
 10  319 ms    380 ms    *         if-1-2.tcore1.L78-London.as6453.net [80.231.130.121]
 11  *         337 ms    *         if-17-2.tcore1.LDN-London.as6453.net [80.231.130.130]
 12  *         *         290 ms   195.219.83.102
 13  284 ms    332 ms    497 ms   v1-3604-ve-228.csw2.London1.Level13.net [4.69.166.102]
```

During routing, each router reduces packets\' TTL value by

- A. 3
- B. 1
- C. 4
- D. 2

Correct Answer: B

Reference: <http://www.packetu.com/2009/10/09/traceroute-through-the-asa/>

QUESTION 13

Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.

Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.

Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.

Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

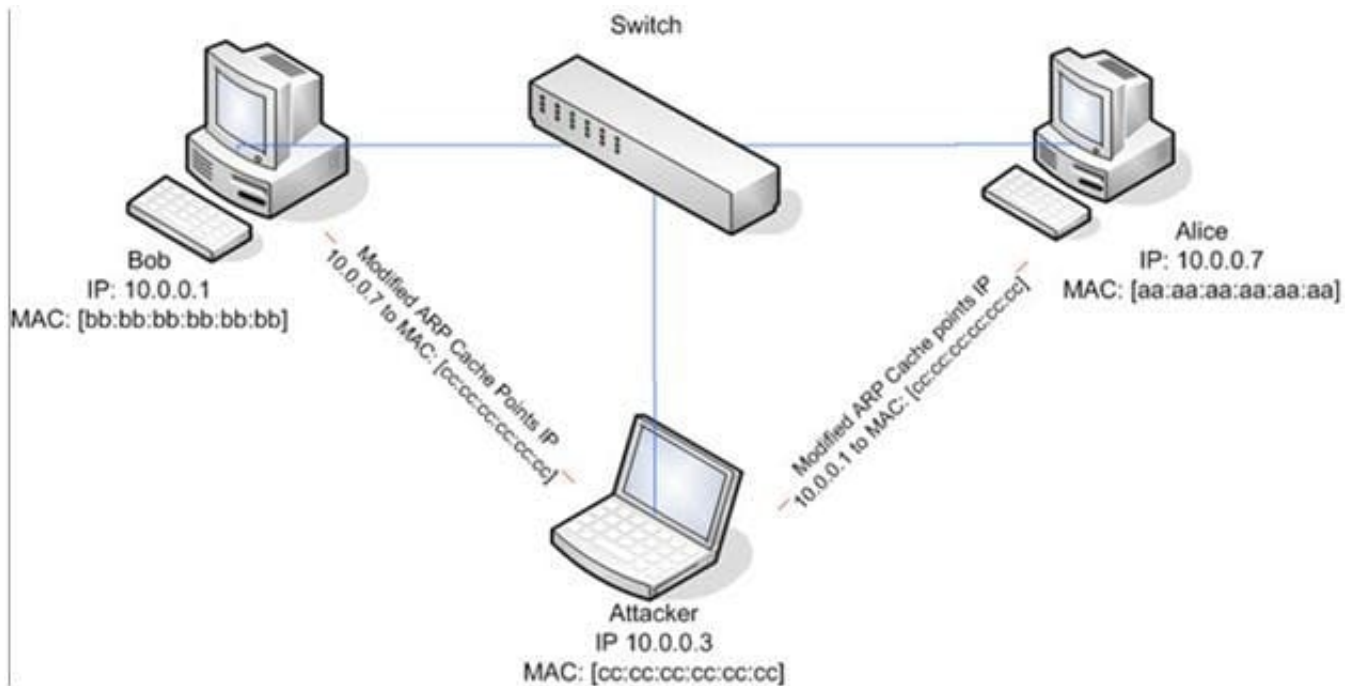
- A. Clever Fuzz Testing
- B. Dumb Fuzz Testing
- C. Complete Fuzz Testing
- D. Smart Fuzz Testing

Correct Answer: C

QUESTION 14

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

- A. Parameter Filtering
- B. Social Engineering
- C. Input Validation
- D. Session Hijacking

Correct Answer: D

Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 15

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. Progressive IDS
- D. NIPS

Correct Answer: B